International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 3, Jun 2014, 159-170

TRANS STELLAR
▪ Journal Publications ▪ Research Consultancy

DIGITAL DATA ENCRYPTION USING MODIFIED METHOD FOR POINT OPERATIONS IN ECC USING MATLAB

MOHAMMED F. ALBRAWY[1], RASHEED M. EL-AWADY[2] & ALI E. TAKI EL_DEEN[3]

[1]Department of Communications and Electronics, Mansoura University, Daqahlia, Egypt

[2]IEEE Senior Member, Department of Communications and Electronics, Mansoura University, Daqahlia, Egypt

[3]IEEE Senior Member, Alexandria University, Daqahlia, Egypt

ABSTRACT

In recent years, Data security has become a priority for any successful information system that can be relied upon to secure its private data in the digital world around us. This depends on the strength of the technique used to secure these data. Elliptic curve cryptography (ECC) has gained Elliptic Curve Cryptography has gained great fame in the field of encryption and security of information because of its strength and speed in data encryption and is what led him to include it in the international standards for information security. A new technique is surveyed to perform point operations multiplication, addition and doubling using MATLAB. The New technique depends on calculating the mathematical expression of point addition and doubling in a faster way. Images and text are the data used to apply the ECC's new technique and the results were satisfactory.

KEYWORDS: Encryption, ECC, Decryptions, Point Operation, Point Addition, Point Doubling and Public Key

INTRODUCTION

Encryption can be defined as the science of secure data through communication systems using mathematical systems have been designed and its analysis technique using simulation and analysis software for digital systems, which is studying the extent of the security system in the presence of Intruders. The four fundamental objectives of secure communications that must be achieved to perform the security goal are Confidentiality, Data integrity, Data origin authentication, Entity authentication and Nonrepudiation. But, Cryptographic systems can be broadly divided into two types Symmetric-key schemes like (DES, RC4, Blowfish and AES) Asymmetric-key schemes like (RSA, ElGamal, ECC).

Elliptic Curve Cryptography is a public key cryptosystem that derives its strength from being dependent on the one-way function it uses. Scalar multiplication is the function that ECC and derivation the inverse of the one-way function is almost intractable to any powerful computing system.

The beginning of the algorithm was in 1985 when Neal Koblitzand Victor Miller submitted a proposal using elliptic curves to design a system for encryption. Since that time a lot of researches have been providing in this area and modifications to improve the performance of that system. This paper is offering one of these improvements to increase the speed of software implementation of the elliptic curve algorithm. In the late 1990's, elliptic curve systems started receiving commercial acceptance when accredited standards organizations specified elliptic curve protocols, and private companies included these protocols in their security products. [1]

There are no algorithms with time sub-exponential to the discrete logarithm problem over elliptic curves. The best known algorithm to date has exponential time. Sum of points on elliptic curve is a slow process if compared with exponentiation modulo a prime in traditional algorithms. However, at the same time of slowness there is the complexity of the discrete logarithm problem that achieves the same level of security with its smaller key.

MATHEMATICAL CONCEPTS

The difficulty and complexity of Elliptic Curve Discrete Logarithm Problem (ECDLP) enabled the system to achieve the required security on groups of points over Elliptic Curve, while sub-exponential algorithms are suitable for solving the integer factorization problem, only exponential algorithms are known for the ECDLP [7]. That is what makes the elliptic curve algorithm better, depending on shorter key size with the same level of security for the information and the most important is its computation efficiency if compared other mathematical algorithms.

Elliptic Curves

An elliptic curve takes the general form as:

$$E: y^2 = x^3 + ax + b \quad (1)$$

Where x, yare co-ordinates of Galois Field GF (p), and a, b are integer modulo p, satisfying

$$4a^3 + 27b^2 \neq 0 \pmod{p}, \quad (2)$$

Where p is a modular prime integer which makes the EC of a finite field. An elliptic curve E over GF (p) consist of the points (x, y) defined by Equations (1) and (2), along with an additional point called O (point at infinity) in EC.

Elliptic Curves over Finite Fields

It can be considered an elliptic curve defined over a finite field, which will turn out to have a finite number of points, which can be in fact bounded. The set of all the points on E is denoted by E (Fp). For example, if E is an elliptic curve over F_5, $F_{11}$and $F_{541}$with defining equation

$$y^2 = x^3 + 2x + 4, \quad (3)$$

To find solutions of equation 3 in F_5, just consider x = 0, 1, 2, 3, 4 and take square roots to find the corresponding y's. The results were as follows and shown in figure 1:

$E(F_5) = \{(0,2), (0,3), (2,1), (2,4), (4,1), (4,4)\}$.

The same is when solving equation 3 in p = 11 and results is shown figure 2:

$E(F_{11})=\{(0,2),(0,9),(2,4),(2,7),(3,2),(3,9),(6,1),(6,10),(7,3),(7,8), (8,2),(8,9),(9,5),(9,6),(10,1),(10,10)\}$

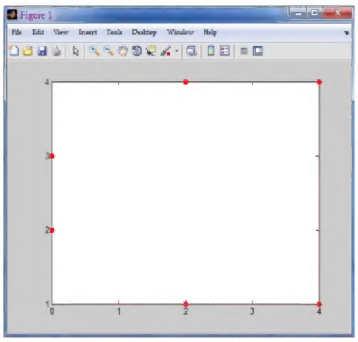


Figure 1: Points of Elliptic Group at p=5

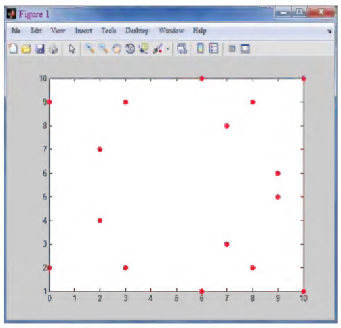


Figure 2: Points of Elliptic Group at p=11

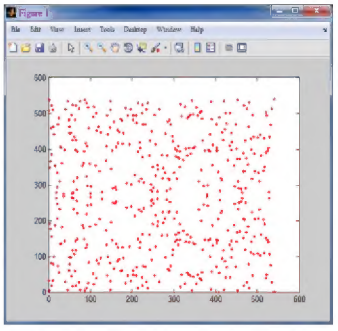


Figure 3: Points of Elliptic Group p=541

Now, there is no problems if a higher value p is chosen, let's use 541. All possible points which makes left side equals right side in equation 3 are shown in figure 3.

If E is an elliptic curve over F_7 and F_{13} with defining equation

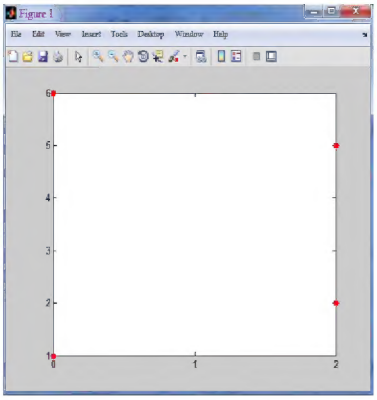
$$y^2 = x^3 + x + 1, \quad (3)$$

then the points on E are

$E(F_7) = \{(0, 1), (0, 6), (2, 2), (2, 5)\}$

$E(F_{13}) = \{(0,1),(0,12),(1,4),(1,9),(4,2),(4,11),(5,1),(5,12),(7,0),(8,1),(8,12),(10,6),(10,7),(11,2),(11,11),(12,5),(12,8\}$

Figure 4 and Figure 5 show the output of elliptic group at p=7 and p=13.



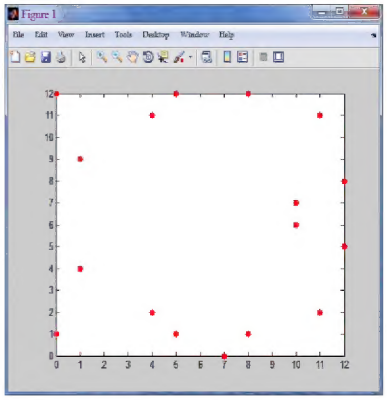


Figure 4: Points of Elliptic Group at p=7 **Figure 5: Points of Elliptic Group at p=13**

Elliptic Curve Arithmetic

Point addition and point doubling are the basic EC operations. ECC primitives [2] require scalar point multiplication. Let P be a point with the coordinates x, y on an EC, and one needs to compute nP, where n is a positive integer.

This scalar multiplication can be done by a series of doubling and addition of P. So, if two points are added $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ then $P_1 + P_2 = P3(x_3, y_3)$ with $P_i = (x_i, y_i) \in E$. Now, there is a well-known method for adding two elliptic curve points (x_1, y_1) and (x_2, y_2) to produce a third point on the elliptic curve.

There are two formulas to compute P_3:

1) $P_1 = P_2$

$$\lambda = \frac{3x_1^2 - a}{2y_1} \bmod p \quad (4)$$

$$x_3 = \lambda^2 - 2x_1 \bmod p \quad (5)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p \quad (6)$$

2) $P_1 \neq P_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod p \quad (7)$$

$$x_3 = \lambda^2 - x_1 - x_2 \bmod p \quad (8)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p \quad (9)$$

Figure 6: Describes the Process of Adding Two Different Points on an Elliptic Curve

Elliptic Curve Point Multiplication

EC point multiplication is the operation of successively adding a point along an elliptic curve to itself repeatedly. It is used in elliptic curve cryptography (ECC) as a means of producing a trapdoor function. The literature presents this operation as scalar multiplication, thus the most common name is "elliptic curve scalar multiplication", as written in Hessian form of an elliptic curve.

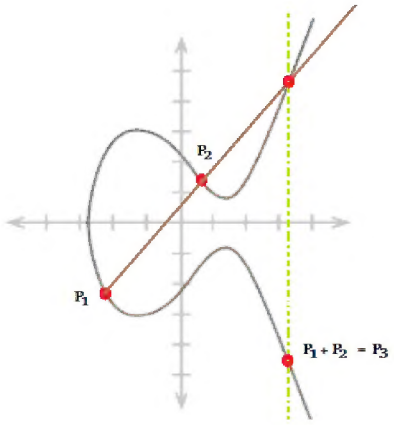


Figure 6: Adding Two Points on an Elliptic Curve

In spite of multiplication or exponentiation in a finite field, ECC uses scalar multiplication. Solving Q = nP (utilized by ECC) is more difficult than solving factorization (used by RSA) and discrete logarithm (used by Diffie-Hellman (DH), EIGamal, Digital Signature Algorithm (DSA)). So ECC is much stronger than other public key agreement and signature authentication methods. [6]

So, ECC depends on the intractability of determining n from Q= n P has given known values of Q and P. It is known as the elliptic curve discrete logarithm problem.

There are two types of n for point multiplication:

- n is a power of two> 1.

- n is any other integer> 1.

First type is the basis to be depended on to perform the new technique to speed up the process point doubling or multiplication.

If n is a power of two, which means the value of n is 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, ……., 2r.So, Q=2P equals Q= P + P which means that the first formula will be used in two point addition. The same will be done if r equal 2 or 3 or any integer.

Let:

n = 4:

$Q = 4\,P$

$Q = 2 \times 2\,P$

n = 8:

$Q = 8\,P$

$Q = 4 \times 2\,P$

$Q = 2 \times 2 \times 2\,P$

n = 32:

$Q = 32\,P$

$Q = 16 \times 2\,P$

$Q = 8 \times 2 \times 2\,P$

$Q = 4 \times 2 \times 2 \times 2\,P$

$Q = 2 \times 2 \times 2 \times 2 \times 2\,P$

And so on for any value of n. Performing point multiplication with doubling is quite difficult and will take a long time in software. But the new technique depended on express value of n in its binary form.

If n equal $(4)_{10}$, so in binary form it will be $(100)_2$ which indicates the number of addition and doubling. Number of doubling processes equal to the number of one's except the first one that is corresponding to 2^0. While, addition processes are equal to the number of one's minus 1.

At n = 4, the number of one's = 1 which means that number of doubling process is one and number of addition process is zero.

Let: P = (5, 16), a = 2, p = 17

Table 1: Result of Doubling Process and Established Time

Multiplication	Doubling	Q	Time (Sec)
2 P	2×P	(6, 14)	0.000559
4 P	2×2×P	(3, 16)	0.000783
8 P	2×2×2×P	(13, 10)	0.000971
16 P	2×2×2×2×P	(10, 6)	0.001142
32 P	2×2×2×2×2×P	(16, 13)	0.001466
64 P	2×2×2×2×2×2×P	(0, 11)	0.001632
128 P	2×2×2×2×2×2×2×P	(9, 16)	0.001915

The previous table presents the value of Q when n is a power of two which induce the only process performed here is doubling process without addition.

The second type is based on first type, but exceeds addition process after doubling process. While Q = n P and n is any integer, the same is done and convert that integer to binary. As mentioned before, the number of ones in binary form shows the number of addition processes and doubling processes. Let us consider n = 3 and its binary representation is $(11)_2$. From binary form, the number of one's is two which means there are one addition process and one doubling process.

Let:

n = 3:
Q = 3 P
Q = P + 2 P

n = 9:
Q = 9 P
Q = P + 8 P
Q = p + (2 × 2× 2 P)

n = 127:
Q = 116P
Q = P+126P
Q = P+2P+124P
Q = P+2P+4P+120P
Q = P+2P+4P+8P+112P
Q = P+2P+4P+8P+16P+96P
Q=P+2P+4P+8P+16P+32P+64P

For n = 9, the binary value is $(1001)_2$ which has two ones, one of them corresponds 2^0. So, doubling processes are only one and two addition processes.

Let: P = (7, 9), a = 1, p = 61

Table 2: Doubling and Addition Results with its Established Time

Multiplication	Doubling	Q	Time (Sec)
3P	P+2P	(21, 30)	0.000631
15P	P+2P+4P+8P	(20, 58)	0.001695
22P	2P+4P+16P	(43, 39)	0.002068
51P	P+2P+16P+32P	(29, 2)	0.002776
85P	P+4P+16P+64P	(18, 13)	0.003215
116P	4P+16P+32P+64P	(1, 48)	0.003474
231P	P+2P+4P+32P+64P+128P	(53, 8)	0.003921

THE ARCHITECTURE OF ELLIPTIC CURVE

There are a lot of things that must be taken into consideration during the implementation of the algorithm in real world applications, such as smart cards and mobile phones, which is the amount of resources would be consumed by the system in addition to the amount of energy consumed. So, low power is the base to design and implement the system. Computation speed is a secondary criteria, in addition to the degree of re-configurability of the device can be kept minimal. [3]

This is because such devices have a short lifetime and are generally configured only once. On the other side of the spectrum, high performance systems such as network servers, database systems, etc. require high speed implementations of ECC.

Now, ECC algorithm will be performed in MATLAB using the new technique and then the overall time established to encrypt and decrypt data will be measured.

Koblitz Method for Encoding Plaintext [4]

Step 1 : Pick an elliptic curve E_p (a, b).
Step 2 : Let us say that E has N points on it.
Step 3 : Let us say that our alphabet consists of the digits
Step 4 : 0,1,2,3,4,5,6,7,8,9 and the letters A, B, C,..., X,Y,Z coded as 10,11,..., 35. And
Step 5 : This converts message into a series of numbers between 0 and 35.
Step 6 : Now choose an auxiliary base parameter
Step 7 : For each number mz (say), take x=mz + i and try to solve for y at i=1.
Step 8 : If no solution for y, then try x = mz +2 and then x = mz +3 until you can solve for y.
Then take the point (x,y). This now converts the number m into a point on the elliptic curve.

As MATAB used step 3 and 4 changes because data used is digital images, then message is now converted to a series of numbers between 0 and 255. If data was in text form, then it is converted according to ASCII table. Also number added to mz replaced by variable i changes from 1 to 20.

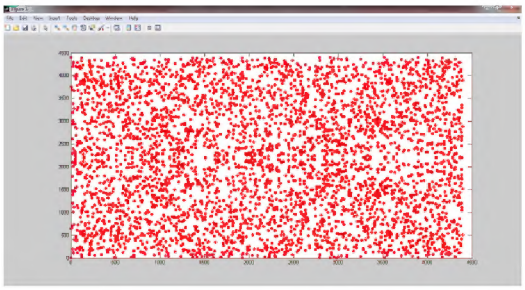


Figure 7: Elliptic Curve Finite Filed at a=1, b=1 and p=4397

Now to decrypt encoded data resulted from koblitz method, there are 3 main steps used to prepare Elliptic curve crypto- system to perform encryption process.

Step 1: Coordinates of Elliptic Curve

In the equation $y^2 = x^3 + ax + b$, let the value of a and b are 1 and 1 respectively, with the value of p= 4397 to find the coordinates of EC in a finite field which shown in figure 7.

Step 2: Elliptic Curve as an Algebraic Structure

There are five properties of elliptic curves, i.e. closure, associative, existence of identity, existence of inverse and commutative, which are required to prove elliptic curve belonging to Abelian group which is implemented in MATLAB generates the coordinates of elliptic curves.

Step 3: Finding all Base or Generator Point

Figure 8: Grey Image Used as Plain Text

The base points or generating points are used in elliptic curve cryptography for public key generation and private key generation. Base points are the points which can generate all the coordinates of an elliptic curve.

Now, each pixel value in the gray image in figure 8 which is our plaintext had been encoded, to a point belong to the finite field which is generated previously in step 2.

SOFTWARE IMPLEMENTATION AND RESULTS

Image Encryption Procedure

Using MATLAB a function created to encode image from its gray scale value of values in elliptic group Figure 9 shows image decoding results. imencode is the function with three input arguments:

Pm= ***imencode***(A, B, EG)

where:

A:	Original image.
B:	The value of z in step 6 in Koblitz's Method for Encoding Plaintext.
EG:	Elliptic curve finite field Group

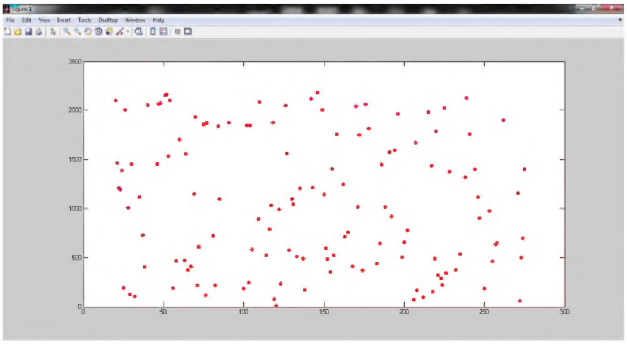


Figure 9: Decoding Image as Points of Elliptic Group

Number of points in the plot not equal to the number of pixels because every red point may contain hundreds of equal points of the same value of x and y but each value is a point in the Elliptic Curve finite field. These points are becoming the encoded plaintext and ready to be decrypted.

After that base point or generating point for generating elliptic curve has to be found to be used in the creation of public with private which user select interval [1, 1-P] according to the following relation:

For USER1:

Private Key = K1

Public Key = PK1 = BP × K1

For USER2:

Private Key = K2

Public Key= PK2 = BP × K2

where: USER1 and USER2 are both agree on Base Point.

It should be noted that the public key generated needs to be validated to ensure that it satisfies the arithmetic requirement of elliptic curve public key [5].Where there is a condition in choosing value of K1 and K2, as not any chosen value from interval [1, 1-P] is right. The result of multiplying keys K1 and K2 by any point from Elliptic Group must be the point of that group to deal with.

Now let elliptic group be used with P=4397 shown in figure 7. That group has 4273 pair; users can choose one of which to be the base point. Let the base point be (3258, 3592).Now, users must choose a value of their private keys K1 and K2. Using my MATLAB function RNDShot, available values can be known in the first 3000 values which can be chosen from.

Available values = {1 2 3 4 5 6 8 9 10 12 16 17 18 20 24 32 33 34 36 40 48 64 65 66 68 72 80 96 128 129 130 132 136 144 160 192 256 257 258 260 264 272 288 320 384 512 513 514 516 520 528 544 576 640 768 1024 1025 1026 1028 1032 1040 1056 1088 1152 1280 1536 2048 2049 2050 2052 2056 2064 2080 2112 2176 2304 2560}

USER1 and USER2 selected 1152 and 2560 respectively to be their private keys. Multiplication of the chosen private keys with base point will product each users' public key.

$$PK1 = (3258, 3592) \times 1152$$

$$= (911, 3274)$$

$$PK2 = (3258, 3592) \times 2560$$

$$= (875, 1608)$$

It is clear that the resultant points PK1 and PK2 are two points in elliptic group.

RNDShotis the function created to check available values for users to select keys from according to base point value. The function has 4 input arguments:

RND= ***RNDShot***(BPx, BPy, EG, p)

where:

BPx:	X value of base point
BPy:	Y value of base point
EG:	Elliptic Group finite field Group
p:	The basic prime number

All is needed now is encrypting encoded plaintext using keys 'public, private' and base point.

Ciphertext of elliptic curve cryptography consists of a pair of points. First point resulted from multiplying a random integer k the interval [1, 1-P] by the base point and the second point from adding encoded plaintext Pm to the multiplication of that random with the public key.First point always fixed and doesn't change as the random and base point doesn't change along encryption process. While the second point is variable as Pm changes according to its value of the original data.

For USER1:

PC = [(k×BP), (Pm + k ×PK1)]

For USER2:

PC = [(k×BP), (Pm + k ×PK2)]

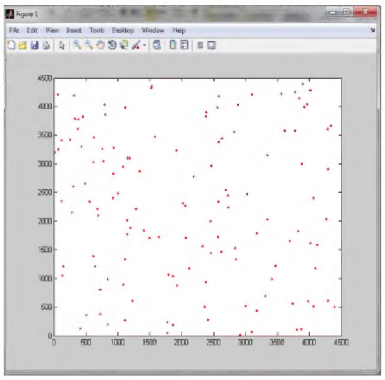


Figure 10: All Values of Ciphertext as Points in EC Group

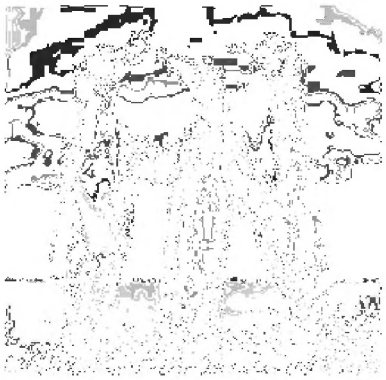


Figure 11: Encrypted Gray Image

USER1 chooses a random number k=2176 and by multiplying it to PK2 then add it to Pm resulted from image encoded. Finally, all values of the second point in ciphertext shown in figure 10 are got where all of these points belong to elliptic group.

Figure 11 shows the output of the ECC algorithm for gray scale image. When the color image shown in figure 13(a) is used as a plain text, time increased about 3 times it takes in gray case to get the ciphertext in figure 13(b).The reason for this is that the color image consists of 3 matrices of red, green and blue, unlike the gray image which consists of a single matrix of gray scale levels.

(a) **(b)**

Figure 13: (a) SharmElshiekh Image as an Original 'Plaintext', (b) Encryption Output 'Ciphertext'

Decryptionoperation

To decrypt ciphertext the keys and parameters established during the encryption process must be used as follows:

Input: The input to the decryption operation is:

- USER2s' private key
- Ciphertext as Pair of points

Processes

- Multiply K2 by the first point.
- Add the result of multiplication to the second point.

Output

- Plaintext as an encoded image.

The final step is decoding output, which would be similar to the points of encoding image shown in figure 10 to get the original image with the same features.

Steps

1- Multiplication.

$K2 \times (k \times BP)$

2- Inverse Addition.

$= (Pm + k \times PK2) – [K2\times (k\times BP)]$

$= Pm + (k \times PK2) – (k \times K2 \times BP)$

$= Pm + (k \times PK2) - (k \times PK2)$

$= Pm$

3- Plaintext deduction.

$m = \frac{Pm - i}{z}$

where i is the value made the equation in step 6 for koblitz method solved for y.

4- Rounds the elements of m toward zero.

Text Encryption Procedure

Same as image encryption, first all texted data are converted to an ASCII code format to start encryption steps. Second, applying function txtencode on the result which convert ASCII value to a corresponding value of the elliptic group.

Plaintext

"We constructed the universe with our own hands, and we are continually expanding it" ~ Quran 51:47

Ciphertext

ৼ֎ৼÅzٍzٍ০□ǸÅ০ৼ০ৼݒৼǸzٍ—□ □ৼ০ݒৼzٍǸ□ৼzٍzٍৼݒÅzٍ□ʧৼÅzٍৼৼÅ□ৼÅzٍzٍ০zٍǸÅ——□ৼ□zٍÅzٍzٍ

□ৼ০ৼৼÛৼ□Ǹ□Åzٍৼ৵Ó৬ৰ৩

Decrypted Text

"We constructed the universe with our own hands, and we are continually expanding it" ~ Quran 51:47

CONCLUSIONS

In this paper, a brief description of ECC key exchange and encryption/decryption has been given. The implementation of ECC on digital image and text document in MATLAB has been explained in detail. Our scheme of encryptionis simple, exploits all security features of elliptic curves and is applicable to all ASCII characters. Since no reference that gives explains scheme of encryption of image and text using ECC in MATLAB has not been coming across, (although there are many references explaining ECC), in addition to that, the new technique used to perform point operation which leads to fast software implementation of mathematical relations. It may be claimed that the scheme described in this paper is our contribution.

REFERENCES

1. Darrel Hankerson, Alfred Menezes and Scott Vanstone "Guide to Elliptic Curve Cryptography", Springer-Verilog 2004.
2. Standard Specifications for Public key cryptography, IEEE Standard, P1363, 2000.
3. Johannes Wolkerstorfer, Hardware Aspects of Elliptic Curve Cryptography, pH. D. Thesis, Institute for Applied Information Processing and Communications, Graz University of Technology, 2004.
4. Padma Bh, D. Chandravathi, P. PrapoornaRoja, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method"(IJCSE)Vol. 02, No. 05, 2010.
5. Randhir Kumar, Akash Anil, "Implementation of Elliptical Curve Cryptography", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011
6. Muhammad Yasir Malik, "Efficient Implementation of Elliptic Curve Cryptography Using Low-power Digital Signal Processor", ISBN 978-89-5519-146-2, Feb. 7-10, 2010 ICACT 2010.
7. S. Maria Celestin Vigila and K. Muneeswaran, "Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications", International Journal of Network Security, Vol.14, No.4, PP.236-242, July 2012.